UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	**No.: 19 CR 980**
vs.	)	
	)	
HAITAO XIANG,	)	
	)	
Defendant.	)	

DEFENDANT'S MOTION TO SUPPRESS EVIDENCE

Table of Contents

Table of Authorities

Supreme Court Cases

Circuit Court and District Court Cases

Statutes

Miscellaneous

I. INTRODUCTION

The failure to obtain a warrant, the lack of suspicion, and the overall unreasonableness relating to the search of Haitao Xiang's electronic devices that were seized at O'Hare Airport require this Court to suppress the evidence found on the devices. Although a warrant was ultimately obtained for these electronic devices, this cannot cure the egregious Fourth Amendment violations that had already occurred. *See, e.g., Brown v. Illinois*, 422 U.S. 590 (1975).

It is improper and deceptive that the search of Mr. Xiang's electronic devices is being masked as a border search, as it is an attempt at a workaround of the Fourth Amendment. The stop and search at O'Hare Airport was not based on any suspicion that the border agents had independently of Mr. Xiang. Rather, they were rooted in an investigation that was initiated by Monsanto and the Federal Bureau of Investigations ("FBI") unrelated to any sort of border security issue. As this Court will see, the FBI contacted Customs and Border Patrol ("CBP") days before Mr. Xiang was apprehended at the airport and before anyone even knew he was planning on flying out of the country.

With the help of CBP, the FBI was able to figure out when and where Mr. Xiang was set to travel. The CBP asked the FBI if they wanted them to seize Mr. Xiang's electronic devices—which they ultimately did. While the government believes that CBP may employ the services of other agencies for assistance, this does not abate the improper actions that the agency it chose for assistance with the alleged border search was not only three hundred miles away—including three hundred

miles away from the FBI offices in Chicago, Illinois much closer to O'Hare Airport—but it was sent to the same agency that was already investigating Mr. Xiang and had contacted CBP about him several days prior.

Despite there being no evidence that Mr. Xiang had committed a crime, he was stopped at O'Hare Airport, had six electronic devices seized, and was ultimately allowed to carry on with his travel. The six seized devices were then passed from CBP to the St. Louis division of the FBI, who were already investigating Mr. Xiang. Without a warrant, these devices were imaged and searched ten days later. The results of the search were then forwarded to Monsanto to confirm whether the found documents were taken by Mr. Xiang without permission, which they confirmed, and this information served as the basis for charges in this matter. This was all done unlawfully and without a warrant. This evidence must be suppressed.

II. RELEVANT FACTS[1]

On May 24, 2017, Mr. Xiang verbally notified Monsanto of his intent to resign. The next day, he submitted his letter of resignation. Mr. Xiang's last day at Monsanto was June 9, 2017, on which day he had an employment exit interview. During the interview, Mr. Xiang stated that he was leaving Monsanto because he had an opportunity that he wanted to pursue. Mr. Xiang indicated that this new opportunity was a joint venture with his PhD advisor at the University of Illinois. This joint venture was through Ag-Sensus which is a National Science Foundation-funded

[1] The Relevant Facts are based on Special Agent Jaret Depke's Affidavit, a June 19, 2017 Federal Bureau of Investigations Report authored by SA Depke, and a July 28, 2017 FBI report authored by SA Depke. Each is attached as exhibits for this Court's review.

startup company that was found to develop and commercialize a near-real-time remote sensing system for agriculture and unmanned aerial system precision farming date management technology. On his termination certification document, Mr. Xiang listed his position at Ag-Sesus as co-founder and chief scientist.

During this interview, Mr. Xiang signed and acknowledged his The Climate Corparation ("TCC") Employment Agreement and Proprietary Information and Inventions Agreement Reminder and TCC Certification. In these documents, Mr. Xiang certified among other things that: "(he) did not have in (his) possession, nor failed to return, any devices, records, data, notes, reports, proposals, lists, correspondence, specifications, drawings, blueprints, sketches, materials, equipment, any other documents or property, or reproductions of any and all aforementioned items belonging to TCC, its subsidiaries, affiliates, successors or assignees." He further agreed that, "in compliance with the At-Will Employment, Confidential Information, Invention Assignment, and Arbitration Agreement, (he) will preserve as confidential all (TCC) Confidential Information and Associated Third Party Confidential Information, including trade secrets, confidential knowledge, data, or other proprietary information relating to products, process, know-how, designs, formulas, developmental or experimental work, computer programs, databases, other original works of authorship, customer lists, business plans, financial information, or other subject matter pertaining to any business of (TCC) or any of its employees, clients, consultants, or licensees."

Also during this interview, when asked if he had copies of company documents

or personal storage devices with company information, Mr. Xiang stated he put all physical documents with company information into the shredder. He also stated he had no storage devices, i.e., USBs or hard drives, with company information. When asked if he had "any Climate/Monsanto confidential business information stored on a private cloud drive anywhere," Mr. Xiang answered, "No." Mr. Xiang was asked if he sent "any confidential information to (his) private email address" to which he answered, "No." When asked if he had any confidential business information on his personal computers at home, he also replied, "No." The interviewers clarified for Mr. Xiang exactly what Climate/Monsanto confidential business information was and Mr. Xiang acknowledged he understood. Mr. Xiang stated he returned all non-public confidential business information in any form. When asked about "storing any Climate/Monsanto data on (his) personal computer" or sharing it with anyone else, Mr. Xiang stated he had not. When asked if he had "transferred or shared any Climate or Monsanto non-public confidential business information, and this includes projects" he worked on or developed himself, Mr. Xiang replied, "No." During this interview, Mr. Xiang also stated he took his Monsanto/TCC work laptop with him on all of his work and personal trips outside of the United States, including his trips to China. When asked if he visited or went on any tours or other agriculture companies or institutions when on personal trips, Mr. Xiang stated that on a personal trip to China in March 2016, he visited the Chinese Science Academy.

Following the exit interview with Mr. Xiang, Monsanto employees informed federal agents that Mr. Xiang appeared to be blatantly deceptive and physically

nervous, especially when he was confronted with what Monsanto employees believed to be suspicious Google searches from 2015 and 2016. On June 8, 2017, Special Agent ("SA") Jaret Depke of the FBI St. Louis ("SL"), coordinated with CBP Task Force Officer ("TFO") Arthur Beck to be notified of international travel by Mr. Xiang and for the possibility of an outbound secondary inspection. SA Depke provided TFO Beck with background information on Mr. Xiang and the circumstances surrounding his resignation at Monsanto. TFO Beck informed SA Depke that he had placed a lockout on Mr. Xiang, including an outbound secondary interview and inspection. TFO Beck asked SA Depke if he wished to request CBP detain any electronics in Mr. Xiang's possession per the Customs Border Search authority and to have the electronics sent to FBI SL for review and analysis. SA Depke informed TFO Beck that he wished to confer with FBI SL Chief Division counsel Craig Stevenson and the U.S. Attorney's Office to ensure the FBI has the appropriate authority to do the above.

That same day, TFO Beck informed SA Depke that Mr. Xiang had scheduled travel from Chicago, Illinois to Shanghai, China on June 10, 2017. On June 9, 2017, SA Depke learned that Mr. Xiang rented a Hyundai Accent from the Avis/Budget Rent a Car in St. Louis, Missouri and on the morning of June 10, 2017, Mr. Xiang dropped off the rented vehicle in Chicago, Illinois.

As Mr. Xiang proceeded to board his flight, he was met on the jetway of the Chicago O'Hare International Airport by a Department of Homeland Security Customs and Border Protection ("DHS-CBP') agent. The DHS-CBP agents conducted an outbound border search of Mr. Xiang's checked and carry-on baggage. The search

revealed the following electronics which were detained by DHS-CBP: (1) a Lenovo Ideapad 1105-11IBR laptop computer, (2) an AT&T Sim Card, (3) an H2O wireless 4G LTE Smart Sim ACT FAST, (4) a Bionex Solution Inc. Thumb Drive, (5) a Samsung Galaxy S5, and (6) a Toshiba 32 Gigabyte Micro SD Card. During the search, Mr. Xiang told DHS-CBP agents that he was traveling to China for one month to visit his parents and vacation. He also told them he had not purchased a return flight to the United States.

Three days later, on June 13, 2017, SA Depke took custody of the devices and secured them in a locked cabinet at the FBI's St. Louis Division office. For some reason, CBP requested that the devices be sent to the FBI's St. Louis Division to be imaged and reviewed. No warrant had yet been obtained.

On June 20, 2017, ten days after the initial seizure of the devices, SA Depke, without a warrant, conducted a preliminary review of the Devices' electronically stored items which had been imaged and prepared for review by the FBI St. Louis Division's Computer Analysis Response Team. SA Depke's review revealed that Monsato documents were on at least one the devises, the Toshiba MicroSD card. At the time of the seizure of the devices from Mr. Xiang, the MicroSD card was attached to the Lenovo laptop. On the MicroSD card, SA Depke identified and reviewed six electronic files, later determined to contain TCC and Monsanto data. Later that same day, agents provided Monsanto employees, familiar with the investigation, copies of these files and documents to determine if they contained Monsanto intellectual property (IP), trade secrets or confidential information.

On June 26, 2017, sixteens days after the seizure of the devices, and six days after the devices were imaged and reviewed, FBI St. Louis Division finally obtained a search warrant authorizing the seizure and examination of the devices and the extraction from that property of electronically stored information.

III. ARGUMENT

There are three separate and independent reasons for this Court to suppress the evidence seized from Mr. Xiang's electronic devices. First, because of the invasive nature of searches of electronic devices that carry in them the most sensitive information an individual has, a warrant must have been obtain to image and search the contents Mr. Xiang's devices. Second, even if a warrant was not required, the agents lacked any articulable suspicion that the electronic devices contained evidence of any sort of crime, whether related to border security or general criminal activity. And third, the search was prolonged and overall unreasonable, clearly weighing the scales in favor of suppression.

This case presents this Court with a rather novel issue, as the Eight Circuit has yet to rule on border searches of electronic devices. *Carpenter* explained that Courts must deal with new technology with the goal of maintaining "that degree of privacy against government that existed when the Fourth Amendment was adopted." *Carpenter v. United States*, 138 S. Ct. 2206, 2214 (2018). The "seismic shifts in digital technology" made searches of data collected by electronic devices less reasonable than more limited-scope physical searches of the same information. *Id.* at 2219. Because electronic devices are "indispensable to participation in modern society" one could not truly opt out of using digital devices and the sensitive

information it gathers. *Id*. at 2206.

Individuals in our society, as exemplified by Mr. Xiang, cannot simply opt out of carrying private information or contraband on his digital devices when he crosses a border. Digital devices are part of modern-day life. People have no real choice in leaving certain data or digital devices at home when they travel. Even if a person deletes files off a device, digital imaging and forensic searches reveal even these deleted files. Many devices give access to data stored in a "Cloud," which is stored in information servers instead of the devices' hard drive. For those reasons, this Court must suppress the evidence found on Mr. Xiang's electronic devices. Not only will it align with the recent advances in Fourth Amendment privacy, but it will also align with the heart of the Fourth Amendment as it was meant to apply from its inception.

A. A WARRANT WAS REQUIRED FOR THE SEARCH OF XIANG'S ELECTRONIC DEVICES

"As the text [of the Fourth Amendment] makes clear, 'the ultimate touchstone of the Fourth Amendment is reasonableness.' " *Riley v. California*, 573 U.S. 373, 382 (2014) (quoting *Brigham City v. Setuart*, 547 U.S. 398, 403 (2006)). When "a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing…reasonableness generally requires the obtaining of a judicial warrant." *Vernonia School Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995). "In the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement." *Riley*, 573 U.S. at 382; *see also Florida v. Royer*, 460 U.S. 491, 500 (1983) ("[A] warrantless search…must be limited in scope to that which is justified by the particular purposes served by the exception."); *United States v, Wurie*,

728 F.3d 1, 3 (1st Cir. 2013) ("[A] warrantless search is *per se* unreasonable under the Fourth Amendment, unless one of 'a few specifically established and well-delineated exceptions' applies").

A search done pursuant to a warrant exception is unreasonable if the search would " 'untether the rule from the justifications underlying' " the exception. *Id*. at 387 (quoting *Arizona v. Gant*, 556 U.S. 332, 343 (2009)). Here, the imaging and search of Mr. Xiang's electronic devices that was conducted jointly by CBP and the FBI and masked as a border search was untethered from the underlying justifications of the border search exception. The search was for combatting general crime unrelated to the border security and was made to further a pre-existing FBI criminal investigation. Ergo, the search falls outside the border exception and was unreasonable without a warrant.

Riley held that the manual search of a cell phone's contents fell outside the search incident to arrest exception because the intrusive search was unrelated to the exception's rationales—officer safety and destruction of evidence. *Id*. at 386. When a court determines "whether to exempt a given type of search" or a "particular category of effect" from the warrant requirement, it must balance "on the one hand, the degree to which it intrudes upon an individual's privacy and on the other, the degree to which it is needed for the promotion of legitimate governmental interests." *Id*. at 385-86. While the exception's two rationales were supported by the search of physical objects, "neither of its rationales ha[d] much force with respect to digital content on cell phones." *Id*. at 385. The Court first analyzed whether either of the rationales were

supported by searching the cellphones, and then analyzed the individual's privacy interest at stake.

Riley ultimately established that an individual has an immense privacy interest in their electronic devices, even when considering the searches at issue were manual searches. *Id.* at 393-97.[2] The cellphones at issue were described as "minicomputers" implying that the computer here carries an even greater privacy interest. *Id.* at 393. The devices "differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person." *Id.* "Before cell phones, a search of a person was limited to the physical realities and tended as a general matter to constitute only a narrow intrusion on privacy." *Id.* But the "intrusion on privacy is not physically limited in the same way when it comes to" electronic devices. *Id.* at 394. The typical cell phone at the time could contain "millions of pages of text, thousands of pictures, or hundreds of videos." *Id.* They also contained certain information that could "reveal much more in combination than any isolated record" and could be used to reconstruct "an individual's private life." *Id.* There is an "element of pervasiveness that characterizes cell phones but not physical records" as it allows a person to carry more personal records on their person than would be in their homes. *Id.* at 395. "Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a person's home." *Id.* at 396. (emphasis original). "A phone not only contains in digital form many sensitive records previously

[2] *Riley* was a consolidation of two cases involving searching a cell phone incident to arrest. *Id.* at 378-79. In both cases, the officers manually searched the phone by looking through the devices themselves without conducting a forensic search. *Id.* at 379-81. As discussed *infra*, a forensic search implicates even greater privacy concerns than in *Riley* and will weigh more in favor of Mr. Xiang.

found in the home; it also contains a broad array of private information never found in a home in any form…" *Id*. at 396-97.

Allowing the officers to search any electronic devices capable of storing records similar to a cell phone, such as Mr. Xiang's hard drive, under the border exception would go against "the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity." *Id*. at 403. "Opposition of such searches was in fact one of the driving forces behind the Revolution itself." *Id*. The mere fact that an individual can now carry the "privacies of life" on his person "does not make the information any less worthy of the protection for which the Founders fought." *Id*. Accordingly, the privacy interests in electronic devices such as cell phones (and hard drives) outweighed any legitimate government interest that were untethered by the search and the Supreme Court imposed the warrant requirement on cell phone searches incident to arrest. *Id*.

As to the rationales underlying the border search exception, the Supreme Court has long recognized that "the Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border." *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004). The justifications for the border exception are the sovereign's interest in "protect[ing]…territorial integrity," nation security interests, and regulating "the entry of unwanted persons and effects." *Id*. at 152-53. Its interest further extends to "regulat[ing] the collection of duties" and "prevent[ing] the introduction of contraband." *United States v. Montoya de*

Hernandez, 473 U.S. 531, 537 (1985); *see also United States v. Ramsey*, 431 U.S. 606, 620 (1977) (the power to conduct warrantless routine searches at the border "is grounded in the recognized right of the sovereign to control, subject to substantive limitations imposed by the Constitution, who and what may enter the country."). "[T]he Supreme Court has identified two principal purposes behind warrantless border searches: First to identify 'travelers … entitled to come in' and, second, to verify their 'belongings as effects which may be lawfully brought in.' " *United States v. Cano*, 934 F.3d 1002. 1013 (9th Cir. 2019) (quoting *Carroll v. United States*, 267 U.S. 132, 154 (1925)).

While courts have extended the justifications underlying the border exception to searches of those exiting the country, *see*, *e.g.*, *United States v. Seljan*, 547 F.3d 993, 999 (9th Cir. 2008); *United States v. Oriakhi*, 57 F.3d 1290, 1296-97 (4th Cir. 1995), the Supreme Court has only framed the justifications for the exception as threats posed at the point of *entry*—not exit. *See*, *e.g.*, *Montoya de Hernandez*, 473 U.S. at 537 ("Since the founding of our Republic, Congress has granted the Executive plenary authority to conduct a routine searches and seizures at the border, without probable cause or a warrant, in order to regulate the collection of duties and to prevent the introduction of contraband into this country"); *United States v. Thirty-Seven Photographs*, 402 U.S. 363, 376 (1971) ("Customs officials characteristically inspect luggage and their power to do so is not questioned…; it is an old practice and is intimately associated with excluding illegal articles from this country"); *Carroll v. United States*, 267 U.S. 132, 154 (1925) ("Travelers may be [stopped and searched] in

crossing an international boundary because of national self-protection reasonably requiring one entering the country to identify himself as entitled to come in, and his belonging as effect which may be lawfully brought in"); *United States v. 12 200-Ft. Reels of Super 8MM Film*, 413 U.S. 123, 93 (1973) (border search authority is justified by the need to prevent smuggling and enforce import restrictions). Because Mr. Xiang was detained at the point of exit, as opposed to entry, the justifications for any sort of border search are diminished. Specifically, the United States surely has an interest in determining the admissibility of persons coming into the country, whereas such interest does not have the same force as applied to those leaving.

To that end, Mr. Xiang's privacy interests in his Lenovo laptop and MicroSD card is immense, dwarfing any legitimate government interest to invasively search the device pursuant to the border exception, particularly to an individual exiting the country. "The average 400-gigabyte laptop hard drive can store over 200 million pages—the equivalent of five floors of a typical academic library." *United States v. Cotterman*, 709 F.3d 952, 964 (9th Cir. 2013). Laptops and hard drives "are simultaneously offices and personal diaries." *Id.* They contain "the most intimate details of our lives: financial records, confidential business documents, medical records and private emails." *Id.* "This type of material implicates the Fourth Amendment's specific guarantee of the people's right to be secure in their 'papers.' " *Id.*; *see also Seljan*, F.3d at 1014 (Kozinski, C.J., dissenting) (The express listing of papers "reflects the Founder's deep concern with safeguarding the privacy of thoughts and ideas—what we call freedom of conscience—from invasion by the government").

Laptops and accompanying hard drives can reveal private information regarding topics such as addiction, religious practices, pregnancy, personal finances, and romance. *Riley*, 573 U.S. at 395-96. Further, the same privacy concerns articulated in *Riley* are applicable here, meaning that the searching an electronic device can provide "far *more*" private information than the most exhaustive search of a house. *Id.* at 396; *see also United States v. Vergara*, 884 F.3d 1309, 1315 (11th Cir. 2018) (J. Pryor, J., dissenting) (pointing out that this proposition in *Riley* is also in light of that fact that a home "historically has received the Fourth Amendment's most stringent protections.").

The information contained in imaged and searched devices seized from Mr. Xiang also differ qualitatively and quantitatively from the types of physical objects traditionally subjected to border searches because electronic devices "are fundamentally different from any object traditionally subject to government searches at the border." *Vergara*, 884 F.3d at 1315 (J. Pryor, J., dissenting). "[T]he sheer quantity of data stored on [electronic devices] dwarfs the amount of personal information that can be carried over a border—and is subjected to a routine border search—in luggage or a car." *United States v. Kolsuz*, 890 F.3d 133, 144 (4th Cir. 2018). As in *Riley*, before cell phone and electronic devices, "border searches were limited by the physical realities that ensured any search would impose a relatively narrow instruction." *Vergara*, 884 F.3d at 1315 (J. Pryor, J., dissenting); *see also Cotterman*, 709 F.3d at 964 ("The amount of private information carried by international travelers was traditionally circumscribed by the size of the traveler's

luggage or automobile"). But with electronic devices, "these physical realities no longer exist." *Id.* Even a car filed to the brim with "sensitive documents cannot hold a candle to the sheer, and ever-increasing, capacity of digital storage." *Cotterman*, 709 F.3d at 964; *see also Kyllo v. United States*, 533 U.S. 27, 33-34 (2001) ("It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology.").

"Subjected to comprehensive forensic analysis, a digital device can reveal an unparalleled breadth of private information." *Kolsuz*, 890 F.3d at 144. Forensic searches are conducted by experts and trained analysts usually at a government forensic laboratory. Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 537 (2005). The examinations can reveal "a wealth of information about how the [device] and its contents have been used." *Id.* at 542. They are also capable of unlocking password-protected files, and retrieving deleted files and browsing histories, meaning that an individual cannot make "meaningful decisions regarding what digital content to expose to the scrutiny that accompanies international travel." *Cotterman*, 709 F.3d at 965. Simply put, "[a] person's digital life ought not be hijacked simply by crossing a border." *Id.*

Applying forensic software to an example of a suitcase, an item that would typically be searched at a border, "it is as if a search of a person's suitcase could reveal not only what the bag contained on the current trip, but everything it had ever carried." *Id.* They are more invasive than the manual searches considered in *Riley*, meaning that "the forensic examination of [electronic devices] should be of even

greater concern given the much more extensive—and more heavily protected from a privacy standpoint—information it may expose." *Vergara*, 884 F.3d at 1316 (J. Pryor, J., dissenting). "A forensic search is far more invasive than any other property search that [the court has] comes across, although it lacks the discomfort or embarrassment that accompanies a body-cavity search, it has the potential to be even more revealing." *United States v. Saboonchi*, 990 F.Supp.2d 536, 568 (D. Md. 2014). While the property is returned at the end of a conventional border search, a forensic search allows law enforcement to conduct a "uniquely probing review not only to the files on one's computer, but also any files that may have been on that computer" and "the search may continue for months or even years afterwards" as law enforcement extract a digital copy of all its contents. *Id.*

This highly intrusive imaging and search of Mr. Xiang's electronic devices was untethered from the justifications of the border search exception. "Border officials are authorized to seize '*merchandise* which … shall have been introduced into the United States in any manner contrary to law." *Cano*, 934 F.3d at 1017 (citing 19 U.S.C. § 482(a)) (emphasis original). "But border officials have no general authority to search for crime" and this proposition is true "even if there is a possibility that such crimes may be perpetrated at the border in the future." *Id.* In *Cano*, CBP discovered 14 kilograms of cocaine inside the defendant's vehicle as he crossed the border from Mexico. *Id.* at 1008. The agents then seized his cell phone and conducted both a manual search and a forensic search. *Id.* The Ninth Circuit held that the manual and forensic searches were untethered from the purposes of the border search exception

because the searches were done to discover evidence of the contraband, not the contraband itself. *Id*. at 117-18. Evidence of contraband "is not itself contraband whose importation is prohibited by law." *Id*. at 1017. "[T]here is no law prohibiting the importation of mere evidence of a crime." *Id*.

The Ninth Circuit described this issue in terms of the scope of the border exception and whether the scope of the exception "include[s] the power to search for *evidence* of contraband that is *not* present at the border." *Id*. (emphasis original). It reasoned that the "detection of contraband is the strongest rationale for the border-search exception." *Id*. at 1018 (citing *United States v. Molina-Isidoro*, 884 F.3d 287, 295 (5th Cir. 2018) (Costa, J., specially concurring). "Every border search case the Supreme Court has decided involved searches to locate *items being smuggled* rather than evidence." *Id*. (emphasis original). The court established that "border officials are limited to searching for contraband only; they may not search in a manner untethered to the search for contraband." *Id*. at 1019. Accordingly, the forensic search of the cell phone was unreasonable under the Fourth Amendment because the agents did not have any suspicion that the cell phone contained contraband.. *Id*. at 1021.

Similarly, in *United States v. Aigbekaen*, a defendant's cell phone, laptop, and media player were forensically searched under the border search exception after law enforcement began investigating the defendant for domestic sex trafficking. 943 F.3d 713, 717-19 (4th Cir. 2019). While the "border search exception to the warrant requirement is broad, it is not boundless." *Id* at 720. The court reasoned that, just as

the search incident to arrest was limited by its underlying justification, so too is the border search exception. *Id.*; *see also Ramsey*, 431 U.S. at 621 (recognizing the similarity between the border exception and the search incident to arrest exception).

Like *Cano, Aigbekaen* recognized that "the Government may not invoke the border exception on behalf of its generalized interest in law enforcement and combatting crime." *Id.* at 721. It recognized that electronic devices "cannot contain many forms of contraband, like drugs or firearms, the detection of which constituted 'the strongest historic rationale for the border search exception.' " *Id.* (quoting *Molina-Isidoro*, 884 F.3d at 295 (Costa, J., specially concurring)). Therefore, the court limited the scope of border searches by requiring that the suspected offense must "bear[] some nexus to the border search exception's purposes of protecting national security, collecting duties, blocking the entry of unwanted persons, or disrupting efforts to export or import contraband." *Id.* "If a nonroutine search becomes too attenuated from these historic rationales, it no longer will all under the exception." *Id.*

There certainly must be – and there is – a limit to the border search exception. The "First Congress authorized customs officials to search for and seize 'goods, wares, and merchandise' that may be concealed in ships entering the country to avoid duties; it did not provide that authority to obtain evidence of crimes other than the contraband itself." *Molina-Isidoro*, 884 F.3d at 295 (Costa, J., specially concurring). "The Supreme Court has long cited that statute … as a reason why warrantless border searches are not 'unreasonable' within the meaning of the Constitution." *Id.* "[T]he modern version of this statute is also limited to the search and seizure of actual

objects that are being imported unlawfully." *Id.* While the strongest historic rationale is the detection of contraband, "[m]ost contraband, the drugs in this case being an example, cannot be stored within the data of a cell phone" and so the "detection-of-contraband justification would not seem to apply to an electronic search of a cell phone or computer." *Molina-Isidoro*, 884 F.3d at 295.

Likewise, a generalized "law enforcement justification is quite far removed from the purpose originally underlying the border exception: protecting this Nation from entrants who may bring anything harmful into the country." *Vergara*, 884 F.3d at 1317. "Excepting forensic [electronic device] searches from the warrant requirement because those searches may produce evidence helpful in future criminal investigation would untether the rule from its justification." *Id.* (citing *Riley*, 573 U.S. at 386). "Unlike physical contraband, electronic contraband is borderless and can accessed and viewed in the United States without ever having crossed a border." *See id.* What CBP and the FBI should have done with Mr. Xiang's electronic devices that were imaged and searched ten days after their seizure is "simple—get a warrant" *Id.* at 1318-19.

It is undeniable that Mr. Xiang had an immense privacy interest in his Lenovo laptop and Micro SD hard drive. For this reason, the forensic imaging and search was a highly invasive intrusion into his privacy interest. And further, the search was not justified by the underlying justifications of the border search exception. This was not a search for contraband authorized by customs laws. Rather it was a general search for evidence of a potential trade secret offense, unrelated to the border. This

is the exact type of situation that the majority of courts have held to untether the border search exception from its justification. *See Aigebekaen*, 943 F.3d at 722 (noting that while the government does have an important general interest in combating crime, this interest does not "categorically eclipse individuals' privacy interests in the vast troves of data contained on their digital devices when the suspected offenses have little or nothing to do with the border."); *City of Indianapolis v. Edmond*, 531 U.S. 32, 41-42 (2000) (when addressing the constitutionality of a checkpoint for narcotics offenses, the Court stated it had "never approved a checkpoint program whose primary purpose was to detect evidence of ordinary criminal wrongdoing" and "without drawing the line at roadblocks designed to serve general interest in crime control, the Fourth Amendment would do little to prevent such intrusions from becoming a routine part of American life"); *see also United States v. Wurie*, 728 F.3d 1, 59 (1st Cir. 2013) (stating in the contents of searching a cell phone incident to arrest that it "found no Supreme Court jurisprudence sanctioning such a general evidence-gathering search"). Allowing federal agencies to use the border exception to search for mere evidence of criminal offenses unrelated to the protection of borders would essentially be granting law enforcement a general warrant at the border to allow investigators to rummage through the most intimate and personal information of any individual, regardless of the reasons. This cannot be.

Digital devices and their contents are borderless. The vast majority of digital information is transferred via the internet. It enters and exits the country without going through a physical border at all. Thus, digital information is not a prevailing

issue that has any effect on security at the border, just as the threat of remote evidence wiping was not a prevailing issue to justify the warrantless searches in *Riley*. Accordingly, a warrantless search of digital devices such as Mr. Xiang's laptop and hard drive cannot be justified under border exception as an individual's privacy interest vastly outweighs the minimum governmental interest.

B. THERE WAS NO REASONABLE SUSPICION TO SUPPORT A WARRANTLESS SEARCH OF XIANG'S ELECTRONIC DEVICES

Should this Court decline to impose a warrant requirement for the search of Mr. Xiang's electronic devices, there still must have been a reasonable suspicion to conduct the non-routine forensic search of Mr. Xiang's electronic devices. "Routine searches of persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant." *Montoya de Hernandez*, 473 U.S. at 19. Routine border searches "are reasonable simply by the virtue of the fact that they occur at the border." *Flores-Montano*, 541 U.S. at 152-53. The Supreme Court, however, has explained that "highly invasive searches" can qualify as "non-routine" and require some level of suspicion. *Id*. at 152. Individualized suspicion is necessary to justify a "highly intrusive search" that infringes upon an individual's "dignity and privacy interest." *Id*. A non-routine border search is only constitutional if based on some level of reasonable suspicion. *See Montoya de. Hernandez*, 473 U.S. at 541. The distinction between routine and nonroutine searches is determined by the degree of invasiveness or intrusiveness of the search. *Molina-Gomez*, 781 F.3d at 19.

Montoya de Hernandez held that an invasive border search of an entrant's person required a reasonable suspicion to be constitutionally upheld. 473 U.S. at 536-

37. Although the government's interest as a sovereign is high at the international border, it must still be balanced against the Fourth Amendment rights of entrants. *Id*. at 539. In *Montoya de Hernandez*, the defendant was suspected of transporting narcotics in her alimentary canal upon landing at LAX from Bogota. *Id*. at 533. The defendant was detained for 16 hours for her to pass the narcotics in her bowl movements. *Id*. at 535-36. The Court balanced her privacy interests and concluded that intrusive searches constitute nonroutine searches that must be supported by a level of suspicion. *Id*. at 537-41.

Building upon the non-routine distinction and using the privacy interests in electronic devices discussed in the section *supra*, the majority of courts have found that forensic searches are nonroutine based on their intrusiveness and have applied some level of suspicion. The Fourth Circuit in *Kolsuz* determined that in light of the privacy interests of cell phones articulated in *Riley*, "a forensic search of a phone must be treated as nonroutine, permissible only on a showing of individualized suspicion." *Kolsuz*, 890 F.3d at 144. Likewise, also due to the highly intrusive nature of an electronic device searches, the Ninth Circuit held that "the forensic search of a cell phone" was nonroutine and imposed a reasonable suspicion standard. *Cano*, 934 F.3d at 1015-16.

Regardless of which approach is taken in regard to the search of Mr. Xiang's electronic devices, there was no objective suspicion that they contained any sort of evidence of a crime, regardless of whether it has a nexus to border security or not. At the time of the search, the only thing SA Depke knew was that Mr. Xiang had quit

his employment at Monsanto, had a one-way ticket to visit his parents in China, and, according to Monsanto employees, acted "deceptive and nervous." Despite the fact that Monsanto employees had no reliability or experience to determine how Mr. Xiang was reacting to their questioning at the exit interview, their observations alone are far from any sort of suspicion that his electronic devices contained evidence of a crime, regardless of whether it was related to border security or not. At the time of the search, there was no evidence or suggestion that Mr. Xiang had downloaded any of Monsanto's confidential documents onto any of those devices; he had answered all of the questions regarding his possession of such documents in the negative, and the emails that he was questioned about were not shown to law enforcement until well after the search of his electronic devices. There was simply nothing to suggest, aside from mere conjecture, that the searched electronic devices had any sort of evidence of a crime. Without such reasonable suspicion, the search was certainly unlawful.

C. THE SEARCH OF XIANG'S ELECTRONIC DEVICES EXCEEDED ANY INITIAL JUSTIFICATION OF A BORDER SEARCH AND UNREASONABLY INFRINGED UPON HIS POSSESSORY RIGHTS IN VIOLATION OF THE FOURTH AMENDMENT

The prolonged, ten-day nature of the search of Mr. Xiang's electronic devices far exceeded the scope and duration of a border search, rending it unreasonable under the Fourth Amendment. In addition to the prolonged search, the invasive nature of the search unreasonably interfered with Mr. Xiang's possessory interests in the electronic devices under the property-based approached. *See, e.g., Molina-Isidoro*, 884 F.3d at 296, n.7 (noting that the property views under the Fourth Amendment "is enjoying a resurgence.").

The Supreme Court explained in *Terry*, that "a search which is reasonable at its inception may violate the Fourth Amendment by virtue of its intolerable intensity and scope." *Terry v. Ohio*, 392 U.S. 1, 18 (1968). Regardless of whether a warrant is required, the Fourth Amendment requires that all search and seizures must be justified at their inception and reasonable in scope and duration. *See United States v. Place*, 462 U.S. 696, 708-09 (1983) ("As we observed in *Terry*, 'the manner in which the seizure was conducted is, of course, as vital a part of the inquiry as whether it was warranted at all.' "); *United States v. Santana-Aguirre*, 537 F.3d 929, 932 (8th Cir. 2008) (explaining that a search done to the consent exception is only reasonable under the Fourth Amendment if the officer does not exceed the scope of consent).

This is true even under the border search exception as "[t]he Fourth Amendment commands that searches and seizures [at the border] be reasonable." *Montoya de Hernandez*, 473 U.S. at 537. In this context, "[w]hat is reasonable depends upon all of the circumstances surrounding the search or seizure and the nature of the search and seizure itself." *Id.* Border searches that are particularly "intrusive" or "offensive" may "be deemed unreasonable under the Fourth Amendment." *Seljan*, 547 F.3d at 1000; *see also Kolsuz*, 890 F.3d at 141 ("The Fourth Amendment protects property as well as privacy and a seizure reasonable at its inception must remain reasonable in scope and duration to satisfy the Fourth Amendment.").

In *Place*, the defendant was stopped and questioned by police in an airport as he was walking towards his gate for a domestic flight from Miami to LaGuardia in

New York. *Place*, 462 U.S. at 698. The defendant gave some remarks that made the police suspicious that he was potentially engaging in some drug courier activities. *Id*. The police informed the DEA in New Yok, and two DEA agents waited for the defendant once his flight arrived. *Id*. The defendant further aroused suspicions that he was carrying narcotics but refused to allow the DEA agents to search his luggage when asked for consent. *Id*. at 698-99. The DEA agents then informed him they were taking his luggage and intended to take the bags to a judge for a search warrant which the defendant could accompany them if desired. *Id*. at 699. The defendant declined but the agents retained the bags and gave the defendant an agent's phone number. *Id*. The agents did not take the luggage to a judge, but rather took the bags to Kennedy Airport where a drug dog conducted a sniff test ultimately leading to the discovery of cocaine. *Id*. A total of 90 minutes had elapsed from the seizure of the bags to the sniff test. *Id*.

The Supreme Court first held that the initial seizure of the luggage was justified under the *Terry* investigatory exception to the Fourth Amendment, because the officers had a reasonable suspicion that he was engaging in criminal activity—transporting narcotics—and law enforcement was justified in seizing the bags to "briefly investigate the circumstances that aroused [their] suspicions." *Id*. at 706. However, the prolonged detention rendered the seizure of the luggage "unreasonable under the Fourth Amendment" absent probable cause. *Id*. at 709-10. Even when initial seizures are justified under an exception to the Fourth Amendment's warrant requirement, a court must "examine whether the agent's conduct…was such as to

place the seizure within the general rule requiring probable cause for a seizure or within *Terry*'s exception to that rule." *Id*. at 708.

The Court further examined the agents conduct and found that it intruded on his possessory interest in his belongings as well as his liberty interest in proceeding with his travel plans. *Id*. "The length of the detention of [the defendant's] luggage alone precludes the conclusion that the seizure was reasonable in the absence of probable cause." *Id*. at 709. Further, "the brevity of the invasion of the individual's Fourth Amendment interests is an important factor in determining whether the seizure is so minimally intrusive as to be justifiable on reasonable suspicion." *Id*. The Court specifically noted that the agents knew the defendant was going to LaGuardia and had "ample time to arrange" other investigative methods there that "could have minimized the intrusion on [the defendant's' Fourth Amendment interest." *Id*. at 709; *see also Royer*, 460 at 500 (when finding that the seizure exceeded the scope of an investigatory stop, the Court stated that it was clear "an investigative detention must be temporary and last no longer than is necessary to effectuate the purposes of the stop" and "the investigative means must be the least intrusive means reasonably available to verify or dispel the officer's suspicion in a short period of time."). Accordingly, the Court ruled that the evidence was inadmissible and reversed the defendant's conviction. *Id*. at 710.

Mr. Xiang's devices were seized for ten days prior to them being imagined and search by SA Depke. This was ample time to obtain a warrant. It took them six days past the search and sixteen after the seizure to obtain one. As this Court knows,

warrants can be obtained within a matter of days, if not the day they are needed. And in the same vein, SA Depke could have imaged and searched the electronic devices the day he received them, not seven days later. This is unreasonable, regardless of where there was probable cause or not (there was none). *See, e.g., Aigbekaen*. at 725, n.10; *United States v. Jacobsen*, 466 U.S. 109, 124 (1984) (even "a seizure lawful at its inception can nevertheless violate the Fourth Amendment because its manner of execution unreasonably infringes possessory interests protected by the Fourth Amendment's prohibition on 'unreasonable searches.' "); *Saboonchi*, 990 F. Supp .2d at 569 (noting that forensic searches of digital devices may deprive individuals of their possessions for periods of days or weeks).

Even when probable cause exists to seize an electronic device – again, there was none here – a significant delay in obtaining a search warrant for the computer was unreasonable under the Fourth Amendment. *United States v. Mitchell*, 565 F.3d 1347, 1353 (11th Cir. 2009). In *Mitchell*, law enforcement became suspicious that the defendant was in possession of child pornography when federal agents discovered that the defendant had purchased a subscription to a child pornography site with his credit card. *Id*. at 1348-49. The agents then visited the defendant at his home where he admitted that he signed up for the site and told them that there was probably child pornography on one of his computers. *Id*. at 1349. The agents then seized the computer and had probable cause to believe it contained child pornography based on the defendant's admissions but did not obtain a search warrant for the computer for another 21 days. *Id*.

While the agents in *Mitchell* were justified with probable cause at the initial seizure of the computer, the search was deemed unreasonable because of the prolonged delay in obtaining the search warrant. *Id*. at 1350-52. Computers are relied upon for personal and business use and they "store personal letters, emails, financial information, passwords, family photos and countless other items of personal nature." *Id*. at 1351. Detaining the computer for three weeks before securing a warrant constituted "a significant interference with Mitchell's possessory interest." *Id*. This is true even though the defendant had a diminished interest in the computer, like a person has a diminished interest at the border, based on his incriminating admissions giving rise to probable cause. *Id*.

Mr. Xiang's interest was not eliminated because his laptop and hard drive were "likely to contain other non-contraband information" and until the agent actually examined the computer, "he cannot be certain that it actually contained" contraband. *Mitchell,* 565 F.3d at 1351. This Court must look at the surrounding facts and circumstances when determining the reasonableness of the delay. *Id*. at 1351.[3] There is absolutely no justification in SA Depke waiting so long both to search the electronic devices and to ultimately obtain a warrant. "[N]o effort was made to obtain a warrant within a reasonable time because law enforcement officers simply believed that there was no rush." *Id*. at 1353. There was no just reason for the delay and therefore the evidence should have been suppressed for violating the Fourth Amendment.

[3] Given that the investigators in *Mitchell* had much stronger and obvious probable cause, the time period for searching or getting a warrant for Xiang's device should be shorter, as investigators did not have probable cause and the initial justification was a narrow exception to the warrant requirement.

Making the search of electronic devices even more unreasonable is that it violated CBP's own policy and exceeded any justifiable scope, further warranting suppression. *See United States v. Laynes*, -- F.Supp.3d -- (S.D. Oh. 2020); Case No. 19-CR-00089; 2020 WL 4901644; *United States v. Kim*, 103 F. Supp .3d 32, 59 (D.D.C. 2015) . In *Layens*, the defendant was a legally admitted resident who arrived at an airport in Ohio following a trip from Mexico. *Id*. at *1. When going through Customs, his fingerprints hit on a "hot list" that indicated he had been convicted of a crime involving moral turpitude at some point, which allowed the agents to determine whether he should be sent to an immigration judge before being admitted. *Id*. at *2. The agents determined that the conviction was remote so there was no need for deferral to a judge, but still decided to examine his cellphone nonetheless. *Id*. The agents made a "manual" search of the cell phone by looking through apps in his phone, and when they found evidence of child pornography in his Google Photos App, they contacted Homeland Security Investigations who then subsequently conducted a forensic search of the phone. *Id*. at *2-*3.

The *Layens* court suppressed the evidence of the searches because it violated the CBP's policy on electronic device searches. *Id*. at *10. It reasoned that law enforcement can only conduct a warrantless search and seizure if they reasonable believed they had the authority to do so and determined that the agents here could not reasonably believe they had authority when it violated its policy. *Id*. at *7-*8; *see also Illinois v. Rodriquez*, 497 U.S. 177, 183-86 (1990) (warrantless search and seizure is permissible if officers reasonably—but erroneously—believed they had been given

permission by a resident to enter the premises).

At the time of the *Layens* search, CBP and DHS issued a policy, *Border Searches of Electronic Devices*, governing how to conduct searches of electronic devices and the scope of such searches. *Id.* at *7. Under the policy, before a manual search—called a basic search in the policy—could be effectuated, the "CBP officials must take steps to ensure that a device is not connected to any network" to avoid accessing data stored remotely. *Id.* The initial searching agent did not place the device in airplane mode or disable network connectivity, which is why he was able to access the images stored on Google Photos, and thereby violated CBP's policy. *Id.* The policy was "clear" and "unequivocally understood" by the agents. *Id.* at *8. The agent's "conduct was not deliberate, but it was in reckless disregard of the border-search policy." *Id.* at *9; *see also Herring v. United States*, 555 U.S. 135, 144 (2009) ("[T]he exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct."). Therefore, the search violated the Fourth Amendment as it was in violation of the CBP's search policies.[4] *Id.* at *10. "[T]o hold otherwise would invite non-compliance with a bright-line requirement put in place by the CBP to comply with Supreme Court precedent." *Id.* at *9.

Evidence derived from the forensic border searches have also been suppressed because the scope of the search was unreasonable based on the minimum suspicion of the agents. *See. Kim*, 103 F. Supp .3d at 59 ("[U]nder the totality of the unique

[4] The district court did not explicitly state that violating the policies rendered the search unreasonable, but it aligns with that reasoning. The search was unreasonable under the Fourth Amendment as it violated and exceeded CBP's own policies on how to conduct border searches.

circumstances of this case, that the imaging and search of the entire contents of [the defendant's] laptop, aided by specialized forensic software, for a period of unlimited duration and an examination of unlimited scope, for the purposes of gathering evidence in a pre-existing investigation, was supported by so little suspicion of ongoing or imminent criminal activity, and was so invasive of [his] privacy and so disconnected from not only the considerations underlying the breadth of the government's authority to search at the border, but also the border itself, that it was unreasonable").

In *Kim*, an HSI agent became suspicious of the defendant of export violations after his nephew became involved in an undercover operation for exporting missile components to Iran and China. *Id*. at 35-37. His nephew informed the undercover agent that his uncle could procure and inspect certain accelerometers and export them from the United States. *Id*. The undercover investigation stalled, and sometime later the nephew was arrested for conspiracy to violate export laws. *Id*. The nephew admitted to investigators that he had previously export similar components from the United States with the help of his uncle. *Id*. at 37-38. Based on this suspicion, the HSI agent planned to seize and search the defendant's computer the next time he left the country, which happened some months after the nephew's arrest. *Id*. at 37-39.

As to the reasonableness of the search, the court was particularly concerned that the agents made an exact digital copy of the defendant's laptop which enabled them to continue searching the laptop for an indefinite duration, even after the laptop was returned. *Id*. at 56-57. "The invasion of privacy was substantial; the agents

created an identical image of [the defendant's] entire computer hard drive and gave themselves unlimited time to search the tens of thousands of documents, images, and emails it contained, using an extensive list of search terms, and with the assistance of forensic programs." *Id*. at 57. The ability to search the digital image of the laptop factored into the reasonableness of the scope of search even though the forensic search started the day after the laptop was seized and concluded approximately five days total after it was seized. *Id*. at 39-41.

Also factoring into the unreasonableness was the location that the forensic search was conducted. *Id*. at 57-58. The laptop was seized at LAX Airport by CBP and a HSI agent, but then sent to HSI forensic computer facility 150 miles away in San Diego. *Id*. at 39-40. The court questioned whether the forensic search was even a border search at all. *See Id*. at 57 ("It is true that [the defendant's] laptop was *seized* at the border…but it was not even opened, much less, searched there.") (emphasis original); *Id*. ("Once the agents had secured the laptop and preserved every single file and folder contained for further examination, how does the examination of the copy and the tens of thousands of emails and other files it contained for the next two weeks fall within the definition of a border search, or the statutory provisions found in 19 U.S.C § 1581(a) at all?"); *see also Aigekaen*, 943 F.3d at 720 ("But this [case] raises another question: Does the border exception even apply to the May 2015 forensic searches?"); *see also Kolsuz*, 890 F.3d at 143 ("At some point, in other words, even a search initiated at the border could become so attenuated from the rationale for the border search exception that it no longer would fall under that exception"). The court

stated that, at best, if the seizing agent "needed the assistance of a forensic team" the initial opening up of the laptop "could arguably be an extension of the border." *Id*. at 57; *see Castillo-Garcia v. United States*, 424 F.2d 482 (9th Cir. 1970) (the term "border" should be given a geographically flexible reading but within the limits of reason derived from the underlying constitutional principles); *Alexander v. United States*, 362 F.2d 379, 382 (9th Cir. 1966) (the legality of a search not in the immediate vicinity of the border "must be tested by a determination of the surrounding circumstances, including the time and distance elapsed.").

The court pointed out several concerns about considering the subsequent search of the digital copy a border search stating that the investigators' testimony "made it clear that the primary, if not sole, purpose of the pre-planned encounter at the border was to obtain the laptop and search it for evidence." *Id*. at 57; *see also Kremen v. United States*, 353 U.S. 346, 347-48 (1957) (holding unconstitutional an exhaustive warrantless search of a cabin, and seizure of its entire contents that were moved 200 miles away for examination). Based on the high invasiveness of the search and the little suspicion that the defendant had engaged in prior border crimes, the seizure and forensic search exceeded the bounds of the initial border seizure and was unreasonable under the Fourth Amendment. *Id*. at 59.

The border search here, much like *Laynes*, violated numerous provisions of CBP's border search policy. The search occurred in 2017 and the effective CBP policy at that time was enacted in 2009.[5] The "Directive governs border search authority,"

[5] U.S. Customs and Border Protection, CBP Directive No. 3340-049, August 20, 2009 (available at https://www.dhs.gov/xlibrary/assets/cbp_directive_3340-049.pdf); *see also Alasaad v. Nielsen*, 419

id. at § 2.3, and it applies to all CBP officials "and other employees authorized by law to perform searches at the border, the function equivalent of the border (FEB), or extended border" and requires all actors to adhere to the directive *Id.* at § 2.2. It stresses that the individual should be present when the search is occurring, unless national security or law enforcement considerations prevent this, and requires that a CBP supervisor be present. *Id.* at §§ 5.1.3-5.1.4.

Section 5.3 governs how the device and data is reviewed and detained as well as assistance from other government agencies. CBP may only "detain electronic devices, or copies of information contained therein, for a brief, reasonable period of time to perform a thorough border search." § 5.3.1. While "the search may take place on-site or at an off-site location" it must still "be completed as expeditiously as possible." *Id.* "[T]he detention of devices ordinarily should not exceed five (5) days." *Id.* Any detention of the device or data beyond the five days must be approved by the Port Director or Patrol Agent in Charge, and any detention exceeding 15 days must be approved by the Director of Field Operations or Chief Patrol Agent. *Id.* at § 5.3.1.1.

Furthermore, CBP must destroy any information extracted from the devices as expeditiously as possible, not to exceed 7 days, unless there is probable cause to seize it. *Id.* at § 5.3.1.2. CBP can only send the device or information to another federal agencies if it needs technical assistance in decrypting, translating, or understanding

F.Supp.3d 142 (D. Mass. 2019) ("Both [DHS and CBP] issued written policies on border searches of electronic devices in August 2009" and CBP updated the policy in January of 2018). The 2018 policy is substantially similar except that the 2018 policy distinguishes procedures between a basic search (a manual search of the device by a person looking through the device) and an advanced search (a search requiring the use of software or external equipment).

the subject matter of the information. *Id*. at §§ 5.3.2.1-5.3.2.2. Importantly, when CBP needs assistance in understanding the subject matter of the device or information, CBP must "have reasonable suspicion of activities in violation of the laws enforced by CBP." § 5.3.2.3. The device itself "should be transmitted only when necessary to render the" assistance, otherwise only a copy of the data should be sent. *Id*. at § 5.3.2.5. Finally, an assisting agency that elects to retain or seize the device or its data may only do so if "it has independent authority." *Id*. at 5.4.2.3.

The Stored Communications Act may also be applicable as under the Act law enforcement cannot obtain access to the contents of scored digital communications from a service provider, such as emails in Mr. Xiang's electronic devices, without first obtaining a warrant issued pursuant to the Federal Rules of Criminal Procedure or by getting a warrant to search his computer. 18 U.S.C. § 2703(a).

The search of Mr. Xiang's electronic devices violated this policy in several ways. First, the CBP and FBI retained the laptop well beyond the five-day period without searching it and, as an assisting agency, the FBI did not search the device as expeditiously as possible. The forensic search did not occur until ten days after CBP seized it at the border, more than double the allotted time allowed. Seemingly, CBP had no intention of meeting its own policy as it seized it and sent it to the FBI upon their request at the inception. This supports that the search was not reasonable in scope or manner as indicated by its own policy. The FBI also had plenty of time to secure a warrant during this prolonged time period but failed to do so for no apparent or legitimate reason. *See United States v. Clutter*, 674 F.3d 980, 984 (8th Cir. 2012)

("Where law enforcement authorities have probable cause to believe that a container holds contraband or evidence of a crime, but have not secured a warrant, the Court has interpreted the Fourth Amendment to permit seizure of the property, *pending issuance of a warrant to examine its contents*, if the exigencies of the circumstances demand it or some other recognized exception to the warrant requirement is present.") (emphasis added); *United States v. Respress*, 9 F.3d 483, 488 (6th Cir. 1993) ("[E]ven with the existence of probable cause to effect a seizure, the duration of the seizure pending the issuance of a search warrant must still be reasonable.").[6]

Second, even if CBP needed the FBI's assistance to understand the information on the electronic devices, the CBP were supposed to send only a copy of the information to the FBI, as they only needed assistance in understanding the subject matter. The CBP has the investigative tools to conduct forensic searches, and even assuming they did not, there are closer FBI and DHS offices in Chicago that could extract the information quicker than it would be than sending the laptop itself to St. Louis, prolonging the search and seizure.

This prolonged seizure indisputably interfered with Mr. Xiang's possessory interests in the devices. There are also doubts on whether CBP would itself had reasonable suspicion that the files could be related to a customs law they were empowered to enforce. The files themselves do not give rise to a reasonably suspicion

[6] Courts have increasingly become critical of law enforcement waiting to obtain warrants given the ease in which technology allows them to obtain them. *See Birchfield v. North Dakota*, --U.S.--, 136 S. Ct. 2160, 2192 (2016) (this "is particularly true in light of 'advances' in technology that now permit 'the more expeditious processing of warrant applications' "; *Cano*, 934 F.3d at 1020 ("Indeed, in most cases the time required to obtain a warrant would seem trivial compared to the hours, days, and weeks needed to complete a forensic search").

of a border crime, and the reasonable suspicion would only arise when the FBI had Monsanto inform them the files were alleged proprietary and trade secrets – well after the search of the electronic devices.

Finally, the CBP violated its policy of allowing the FBI to retain the laptop and data itself because, absent a warrant or consent, the FBI had no authority on its own to seize or extract personal information from a person's laptop. Therefore, on top of the immense privacy concerns of information on laptops, CBP knowingly, or at least recklessly, violated its own policy just to further than investigation of the FBI, not any of their own border-related concerns.

The FBI should not have been conducting the border search at all. "[T]he authorizing statute limits the persons who may legally conduct a 'border search' to persons authorized to board or search vessels." *Cano*, 934 F.3d at 1013. "This includes customs and immigration officials, but not general law enforcement agencies such as FBI agents." *Id.*; *see also United States v. Diamond*, 471 F.2d 77, 773 (9th Cir. 1973) (stating that "customs agents are not general guardians of the public peace"). The searches must also be conducted "in enforcement of customs law" and to "enforce importation laws, not for general law enforcement purposes." *Id.* "A general search cannot be justified on the mere basis that it occurred at the border." *Id.* Even if the FBI could conduct the border search, the search of Mr. Xiang's electronic devices was obviously to further the FBI's 'general law enforcement purpose' and was attenuated from the actual justification of the border searches. Clearly, the FBI was exploiting the border search exception for its own purposes, and thereby exceed the initial

justification of the search.

And much like *Kim,* the search exceeded the scope of the initial border search and was an unreasonable means of conducting the search. A border search is a narrow, limited exception to the warrant requirement. It does not authorize the exceedingly intrusive forensic search that occurred on Mr. Xiang's electronic devices, especially when the only suspicion was a nervous exit interview and suspect Google searches that the FBI did not even see until after the search. The CBP policy was specifically implemented to make sure that border searches were reasonable and complied with Supreme Court precedent. And yet it repeatedly violated the policy for the purposes of giving the FBI unbridled access to the most personal aspects of Mr. Xiang's private life. CBP seized the computer on behalf of the FBI and transported it 300 miles, to another state, just to serve that FBI office's investigative goals in their investigation of Mr. Xiang based on unsupported claims from Monsanto. There is grave concern whether this search was actually a border search at all, let alone a reasonable one.

CONCLUSION

There is no justification for the intrusive searches of Mr. Xiang's seized electronic devices. Not only was the search warrantless, suspicionless, and overall unreasonable, but the deceptive action of the FBI to mask it as a border search is disingenuous, to say the least. Nothing about this search was related to border security but was backdoored as such to avoid the Fourth Amendment requirements the FBI would have had to otherwise maneuver in order to lawfully investigate its

case. This Court must hold the government to the standards imposed upon them by the United States Constitution and suppress the evidence the was obtained as a result of the wanton disregard for Mr. Xiang's rights.

Respectfully submitted,

/s/ Vadim A. Glozman
An Attorney for Haitao Xiang

Vadim A. Glozman
LAW OFFICES OF VADIM A. GLOZMAN
53 W. Jackson Blvd., Suite 1410
Chicago, IL 60604
(312) 726-9015

Eric M. Selig
Law Office of Eric Selig
222 S. Central Suite 1004
Clayton, MO 63105
Tel: 314-609-3542

CERTIFICATE OF SERVICE

I hereby certify that on February 19, 2021, a true and correct copy of the foregoing was filed electronically with the Clerk of the Court to be served by operation of the Court's electronic filing system upon the following: all Attorneys of record.

s/ Vadim A. Glozman